Exhibit K

GLOBAL EDITION
The New York Times
WITH THE International Herald Tribune

You for Sale: Mapping, and Sharing, the Consumer Genome

By NATASHA SINGER
Published: June 16, 2012

IT knows who you are. It knows where you live. It knows what you do.

t peers deeper into American life than the F.B.I. or the I.R.S., or those prying digital eyes at Facebook and Google. If you are an American adult, the odds are that it knows things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams — and on and on.

Right now in Conway, Ark., north of Little Rock, more than 23,000 computer servers are collecting, collating and analyzing consumer data for a company that, unlike Silicon Valley's marquee names, rarely makes headlines. It's called the Acxiom Corporation, and it's the quiet giant of a multibillion-dollar industry known as database marketing.

Few consumers have ever heard of Acxiom. But analysts say it has amassed the world's largest commercial database on consumers — and that it wants to know much, much more. Its servers process more than 50 trillion data "transactions" a year. Company executives have said its database contains information about 500 million active consumers worldwide, with about 1,500 data points per person. That includes a majority of adults in the United States.

Such large-scale data mining and analytics — based on information available in public records, consumer surveys and the like — are perfectly legal. Acxiom's customers have included big banks like Wells Fargo and HSBC, investment services like E*Trade, automakers like Toyota and Ford, department stores like Macy's — just about any major company looking for insight into its customers.

For Acxiom, based in Little Rock, the setup is lucrative. It posted profit of $77.26 million in its latest fiscal year, on sales of $1.13 billion.

But such profits carry a cost for consumers. Federal authorities say current laws may not be equipped to handle the rapid expansion of an industry whose players often collect and sell sensitive financial and health information yet are nearly invisible to the public. In essence, it's as if the ore of our data-driven lives were being mined, refined and sold to the highest bidder, usually without our knowledge — by companies that most people rarely even know exist.

Julie Brill, a member of the Federal Trade Commission, says she would like data brokers in general to tell the public about the data they collect, how they collect it, whom they share it with and how it is used. "If someone is listed as diabetic or pregnant, what is happening with this information? Where is the information going?" she asks. "We need to figure out what the rules should be as a society."

Although Acxiom employs a chief privacy officer, Jennifer Barrett Glasgow, she and other executives declined requests to be interviewed for this article, said Ines Rodriguez Gutzmer, director of corporate communications.

In March, however, Ms. Barrett Glasgow endorsed increased industry openness. "It's not an unreasonable request to have more transparency among data brokers," she said in an interview with The New York Times. In marketing materials, Acxiom promotes itself as "a global thought leader in addressing consumer privacy issues and earning the public trust."

But, in interviews, security experts and consumer advocates paint a portrait of a company with practices that privilege corporate clients' interests over those of consumers and contradict the company's stance on transparency. Acxiom's marketing materials, for example, promote a special security system for clients and associates to encrypt the data they send. Yet cybersecurity experts who examined Acxiom's Web site for The Times found basic security lapses on an online form for consumers seeking access to their own profiles. (Acxiom says it has fixed the broken link that caused the problem.)

In a fast-changing digital economy, Acxiom is developing even more advanced techniques to mine and refine data. It has recruited talent from Microsoft, Google, Amazon.com and Myspace and is using a powerful, multiplatform approach to predicting consumer behavior that could raise its standing among investors and clients.

Of course, digital marketers already customize pitches to users, based on their past activities. Just think of "cookies," bits of computer code placed on browsers to keep track of online activity. But Acxiom, analysts say, is pursuing far more comprehensive techniques in an effort to influence consumer decisions. It is integrating what it knows about our offline, online and even mobile selves, creating in-depth behavior portraits in pixilated detail. Its executives have called this approach a "360-degree view" on consumers.

"There's a lot of players in the digital space trying the same thing," says Mark Zgutowicz, a Piper Jaffray analyst. "But Acxiom's advantage is they have a database of offline information that they have been collecting for 40 years and can leverage that expertise in the digital world."

Yet some prominent privacy advocates worry that such techniques could lead to a new era of consumer profiling.

Jeffrey Chester, executive director of the Center for Digital Democracy, a nonprofit group in Washington, says: "It is Big Brother in Arkansas."

SCOTT HUGHES, an up-and-coming small-business owner and Facebook denizen, is Acxiom's ideal consumer. Indeed, it created him.

Mr. Hughes is a fictional character who appeared in an Acxiom investor presentation in 2010. A frequent shopper, he was designed to show the power of Acxiom's multichannel approach.

In the presentation, he logs on to Facebook and sees that his friend Ella has just become a fan of Bryce Computers, an imaginary electronics retailer and Acxiom client. Ella's update prompts Mr. Hughes to check out Bryce's fan page and do some digital window-shopping for a fast inkjet printer.

Such browsing seems innocuous — hardly data mining. But it cues an Acxiom system designed to recognize consumers, remember their actions, classify their behaviors and influence them with tailored marketing.

When Mr. Hughes follows a link to Bryce's retail site, for example, the system recognizes him from his Facebook activity and shows him a printer to match his interest. He registers on the site, but doesn't buy the printer right away, so the system tracks him online. Lo and behold, the next morning, while he scans baseball news on ESPN.com, an ad for the printer pops up again.

That evening, he returns to the Bryce site where, the presentation says, "he is instantly recognized" as having registered. It then offers a sweeter deal: a $10 rebate and free shipping.

It's not a random offer. Acxiom has its own classification system, PersonicX, which assigns consumers to one of 70 detailed socioeconomic clusters and markets to them accordingly. In this situation, it pegs Mr. Hughes as a "savvy single" — meaning he's in a cluster of mobile, upper-middle-class people who do their banking online, attend pro sports events, are sensitive to prices — and respond to free-shipping offers.

Correctly typecast, Mr. Hughes buys the printer.

But the multichannel system of Acxiom and its online partners is just revving up. Later, it sends him coupons for ink and paper, to be redeemed via his cellphone, and a personalized snail-mail postcard suggesting that he donate his old printer to a nearby school.

Analysts say companies design these sophisticated ecosystems to prompt consumers to volunteer enough personal data — like their names, e-mail addresses and mobile numbers — so that marketers can offer them customized appeals any time, anywhere.

Still, there is a fine line between customization and stalking. While many people welcome the convenience of personalized offers, others may see the surveillance engines behind them as intrusive or even manipulative.

"If you look at it in cold terms, it seems like they are really out to trick the customer," says Dave Frankland, the research director for customer intelligence at Forrester Research. "But they are actually in the business of helping marketers make sure that the right people are getting offers they are interested in and therefore establish a relationship with the company."

DECADES before the Internet as we know it, a businessman named Charles Ward planted the seeds of Acxiom. It was 1969, and Mr. Ward started a data processing company in Conway called Demographics Inc., in part to help the Democratic Party reach voters. In a time when Madison Avenue was deploying one-size-fits-all national ad campaigns, Demographics and its lone computer used public phone books to compile lists for direct mailing of campaign material.

Today, Acxiom maintains its own database on about 190 million individuals and 126 million households in the United States. Separately, it manages customer databases for or works with 47 of the Fortune 100 companies. It also worked with the government after the September 2001 terrorist attacks, providing information about 11 of the 19 hijackers.

To beef up its digital services, Acxiom recently mounted an aggressive hiring campaign. Last July, it named Scott E. Howe, a former corporate vice president for Microsoft's advertising business group, as C.E.O. Last month, it hired Phil Mui, formerly group product manager for Google Analytics, as its chief product and engineering officer.

In interviews, Mr. Howe has laid out a vision of Acxiom as a new-millennium "data refinery" rather than a data miner. That description posits Acxiom as a nimble provider of customer analytics services, able to compete with Facebook and Google, rather than as a stealth engine of consumer espionage.

Still, the more that information brokers mine powerful consumer data, the more they become attractive targets for hackers — and draw scrutiny from consumer advocates.

This year, Advertising Age ranked Epsilon, another database marketing firm, as the biggest advertising agency in the United States, with Acxiom second. Most people know Epsilon, if they know it at all, because it experienced a major security breach last year, exposing the e-mail addresses of millions of customers of Citibank, JPMorgan Chase, Target, Walgreens and others. In 2003, Acxiom had its own security breaches.

But privacy advocates say they are more troubled by data brokers' ranking systems, which classify some people as high-value prospects, to be offered marketing deals and discounts regularly, while dismissing others as low-value — known in industry slang as "waste."

Exclusion from a vacation offer may not matter much, says Pam Dixon, the executive director of the World Privacy Forum, a nonprofit group in San Diego, but if marketing algorithms judge certain people as not worthy of receiving promotions for higher education or health services, they could have a serious impact.

"Over time, that can really turn into a mountain of pathways not offered, not seen and not known about," Ms. Dixon says.

Until now, database marketers operated largely out of the public eye. Unlike consumer reporting agencies that sell sensitive financial information about people for credit or employment purposes, database marketers aren't required by law to show consumers their own reports and allow them to correct errors. That may be about to change. This year, the F.T.C. published a report calling for greater transparency among data brokers and asking Congress to give consumers the right to access information these firms hold about them.

ACXIOM'S Consumer Data Products Catalog offers hundreds of details — called "elements" — that corporate clients can buy about individuals or households, to augment their own marketing databases. Companies can buy data to pinpoint households that are concerned, say, about allergies, diabetes or "senior needs." Also for sale is information on sizes of home loans and household incomes.

Clients generally buy this data because they want to hold on to their best customers or find new ones — or both.

A bank that wants to sell its best customers additional services, for example, might buy details about those customers' social media, Web and mobile habits to identify more efficient ways to market to them. Or, says Mr. Frankland at Forrester, a sporting goods chain whose best customers are 25- to 34-year-old men living near mountains or beaches could buy a list of a million other people with the same characteristics. The retailer could hire Acxiom, he says, to manage a campaign aimed at that new group, testing how factors like consumers' locations or sports preferences affect responses.

But the catalog also offers delicate information that has set off alarm bells among some privacy advocates, who worry about the potential for misuse by third parties that could take aim at vulnerable groups. Such information includes consumers' interests — derived, the catalog says, "from actual purchases and self-reported surveys" — like "Christian families," "Dieting/Weight Loss," "Gaming-Casino," "Money Seekers" and "Smoking/Tobacco." Acxiom also sells data about an individual's race, ethnicity and country of origin. "Our Race model," the catalog says, "provides information on the major racial category: Caucasians, Hispanics, African-Americans, or Asians." Competing companies sell similar data.

Acxiom's data about race or ethnicity is "used for engaging those communities for marketing purposes," said Ms. Barrett Glasgow, the privacy officer, in an e-mail response to questions.

There may be a legitimate commercial need for some businesses, like ethnic restaurants, to know the race or ethnicity of consumers, says Joel R. Reidenberg, a privacy expert and a professor at the Fordham Law School.

"At the same time, this is ethnic profiling," he says. "The people on this list, they are being sold based on their ethnic stereotypes. There is a very strong citizen's right to have a veto over the commodification of their profile."

He says the sale of such data is troubling because race coding may be incorrect. And even if a data broker has correct information, a person may not want to be marketed to based on race.

"DO you really know your customers?" Acxiom asks in marketing materials for its shopper recognition system, a program that uses ZIP codes to help retailers confirm consumers' identities — without asking their permission.

"Simply asking for name and address information poses many challenges: transcription errors, increased checkout time and, worse yet, losing customers who feel that you're invading their privacy," Acxiom's fact sheet explains. In its system, a store clerk need only "capture the shopper's name from a check or third-party credit card at the point of sale and then ask for the shopper's ZIP code or telephone number." With that data Acxiom can identify shoppers within a 10 percent margin of error, it says, enabling stores to reward their best customers with special offers. Other companies offer similar services.

"This is a direct way of circumventing people's concerns about privacy," says Mr. Chester of the Center for Digital Democracy.

Ms. Barrett Glasgow of Acxiom says that its program is a "standard practice" among retailers, but that the company encourages its clients to report consumers who wish to opt out.

Acxiom has positioned itself as an industry leader in data privacy, but some of its practices seem to undermine that image. It created the position of chief privacy officer in 1991, well ahead of its rivals. It even offers an online request form, promoted as an easy way for consumers to access information Acxiom collects about them.

But the process turned out to be not so user-friendly for a reporter for The Times.

In early May, the reporter decided to request her record from Acxiom, as any consumer might. Before submitting a Social Security number and other personal information, however, she asked for advice from a cybersecurity expert at The Times. The expert examined Acxiom's Web site and immediately noticed that the online form did not employ a standard encryption protocol — called https — used by sites like Amazon and American Express. When the expert tested the form, using software that captures data sent over the Web, he could clearly see that the sample Social Security number he had submitted had not been encrypted. At that point, the reporter was advised not to request her file, given the risk that the process might expose her personal information.

Later in May, Ashkan Soltani, an independent security researcher and former technologist in identity protection at the F.T.C., also examined Acxiom's site and came to the same conclusion. "Parts of the site for corporate clients are encrypted," he says. "But

for consumers, who this information is about and who stand the most to lose from data collection, they don't provide security."

Ms. Barrett Glasgow says that the form has always been encrypted with https but that on May 11, its security monitoring system detected a "broken redirect link" that allowed unencrypted access. Since then, she says, Acxiom has fixed the link and determined that no unauthorized person had gained access to information sent using the form.

On May 25, the reporter submitted an online request to Acxiom for her file, along with a personal check, sent by Express Mail, for the $5 processing fee. Three weeks later, no response had arrived.

Regulators at the F.T.C. declined to comment on the practices of individual companies. But Jon Leibowitz, the commission chairman, said consumers should have the right to see and correct personal details about them collected and sold by data aggregators.

After all, he said, "they are the unseen cyberazzi who collect information on all of us."

A version of this article appeared in print on June 17, 2012, on page BU1 of the New York edition with the headline: You For Sale.